INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Force Protection Common Operational Picture/Common Tactical Picture

B. DATE Report Downloaded From the Internet 8/13/98

Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **Department of the Air Force**
Hqtrs Electronic Systems Ctr(AFMC)
ATTN: Col Russell N. Peter
(781) 377-6002
5 Eglin Street, Bldg 1624
Hanscom AFB, MA 01731-2308

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

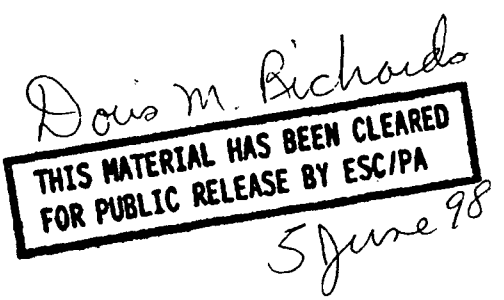
F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: UM **Preparation Date**: 8/13/98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

19980819 077

DTIC QUALITY INSPECTED 1

FORCE PROTECTION
COMMON OPERATIONAL PICTURE / COMMON TACTICAL PICTURE



COLONEL RUSSELL N. PETER, ESC/FD
5 EGLIN STREET
BUILDING 1624
HANSCOM AFB, MA 01731-2308
PHONE: (781) 377-6002
FAX: (781) 377-8832
E-MAIL: peterr@hanscom.af.mil

ESC 98-0549
AQ I98-11-2271

Force Protection Common Operational Picture/Common Tactical Picture

25 June 1996: The Wake Up Call

At 2153 hours local, a truck bomb exploded at the Khobar Towers compound near Dhahran and killed 19 service members. Khobar Towers was the residential quarters of almost 3,000 US military personnel of the 440th Air Wing (Provisional).

William J. Perry, Secretary of Defense, in his Report to the President and Congress on the Protection of U. S. Forces Deployed Abroad on 15 September 1996 said: "...the Khobar Towers attack should be seen as a watershed event pointing the way to a radically new mindset and dramatic changes in the way we protect our forces deployed overseas from this growing threat."

In response to this attack and the growing potential for more attacks by terrorists, irregular forces, and disenchanted employees against its bases and facilities and personnel, the Air Force has taken an integrated approach to Force Protection. There is a recognition that Force Protection is not a Security Police operation; but is a Security Force operation. This exemplifies a mindset change and a movement away from pure law enforcement and stovepipe operations to an integrated Security Force for Force Protection. This is evidenced by the formation last year of the 820th Security Forces Group (SFG) with its mix of security force, office of special investigations (OSI), intelligence, medical, communications, civil engineering, and logistics and supply personnel and the Force Protection Battlelab with a similar mix of personnel. The Air Staff now has a Security Force directorate (SAF/SF) and the Security Forces Center has been established at Lackland AFB, TX.

The threat to our bases and facilities is multi-dimensional. It could manifest itself as a medical attack; an information warfare attack; a chemical, biological, or nuclear weapon attack; a military operation (ground, air, and/or sea attack); a sapper attack; or any combination thereof. In the past, these incidents or attacks would have been reported within stovepipe channels; but, as highlighted by the Downing Report on Khobar Towers which stated there was a requirement for the infusion of intelligence support for Force Protection operations, the Force Protection mission area must have an integrated approach for providing situation awareness to our Security Force elements. These elements must have an understanding of the theater/regional Force Protection (FP) environment for uncommitted forces, as well as a local situation awareness picture, much as is done for the engaged forces within the Global Command and Control System (GCCS) Common Operational Picture. To address this need, the Force Protection C2 Systems program office at Hanscom AFB, MA (ESC/FD) has initiated a proof-of-concept testbed effort modeled after the Common Operational Picture concept - the Force Protection Common Operational Picture/Common Tactical Picture (COP/CTP). (The definitions for the GCCS COP and CTP are attached.)

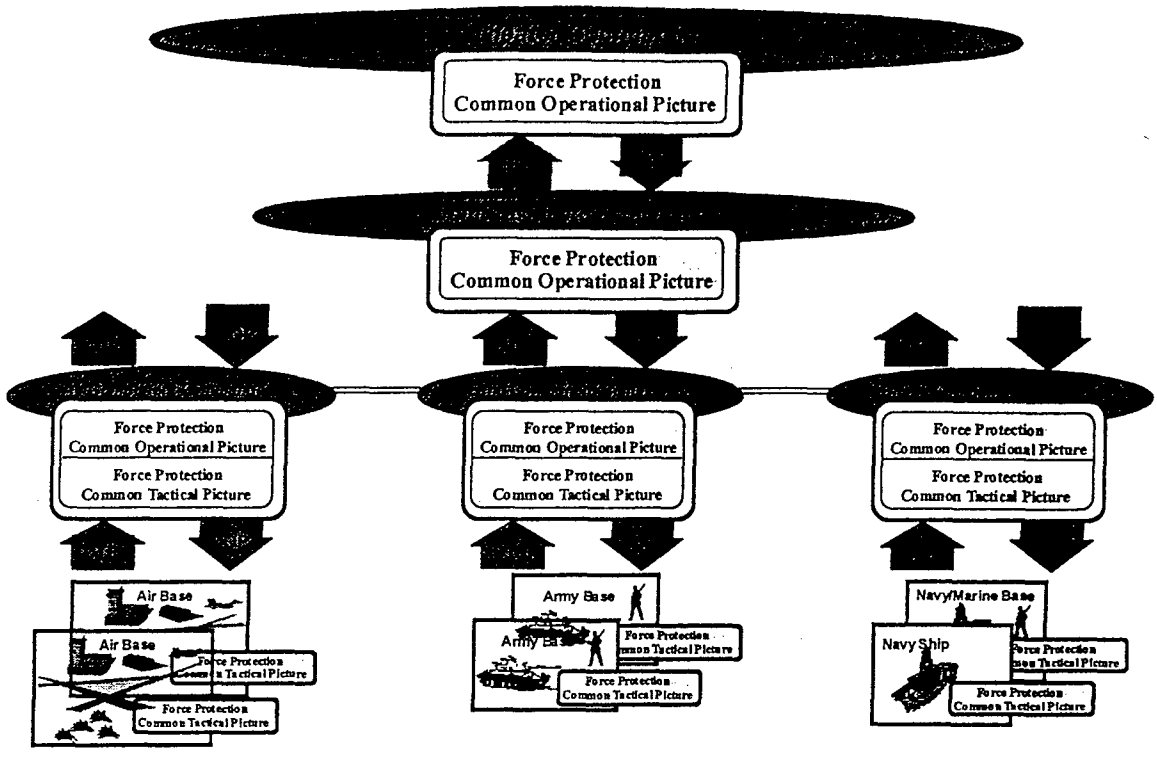


Figure 1: Joint Force Protection Tailored Awareness

Description:

The Air Force Security Forces have established five integrated protection zones around their facilities and personnel in order to characterize protection needs, information flows, and areas of responsibility: airman, perimeter, tactical, detection, and intelligence.

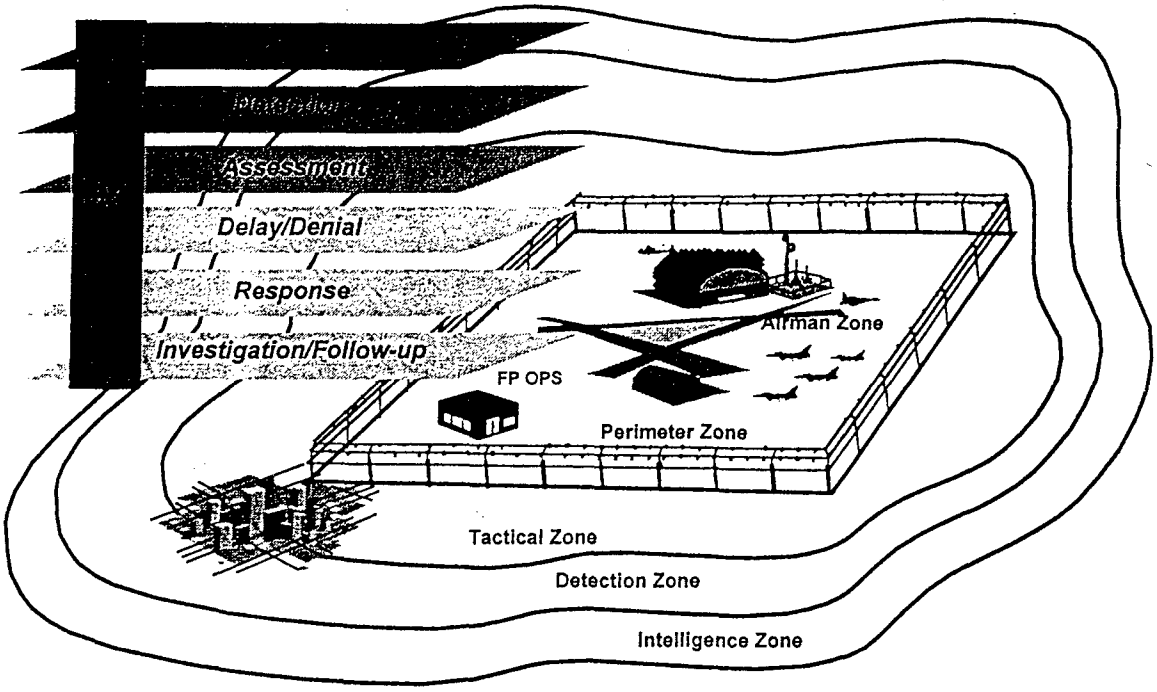


Figure 2: The Force Protection World Tactical View

The FP COP provides a view of the FP intelligence zone. Portrayed are incidents, such as fires, hazardous material detections, kidnappings, intrusions or events at other installations, as well as global trends of activities of terrorist, irregular force, or disenchanted elements. Global weather and global news, as provided by CNN-type organizations and news services, related to the Force Protection mission area are also presented as part of this COP. Additionally, it is envisioned that General Military Intelligence topics of interest, such as new weapons and their functionality and regional terrorist organizational structures, capabilities, and personalities would also be covered as part of the COP. The FP COP would be a joint force product created at the Joint Task Force (JTF)/Theater Commander in Chief (CINC) level and disseminated to the service component security forces throughout the area of responsibility.

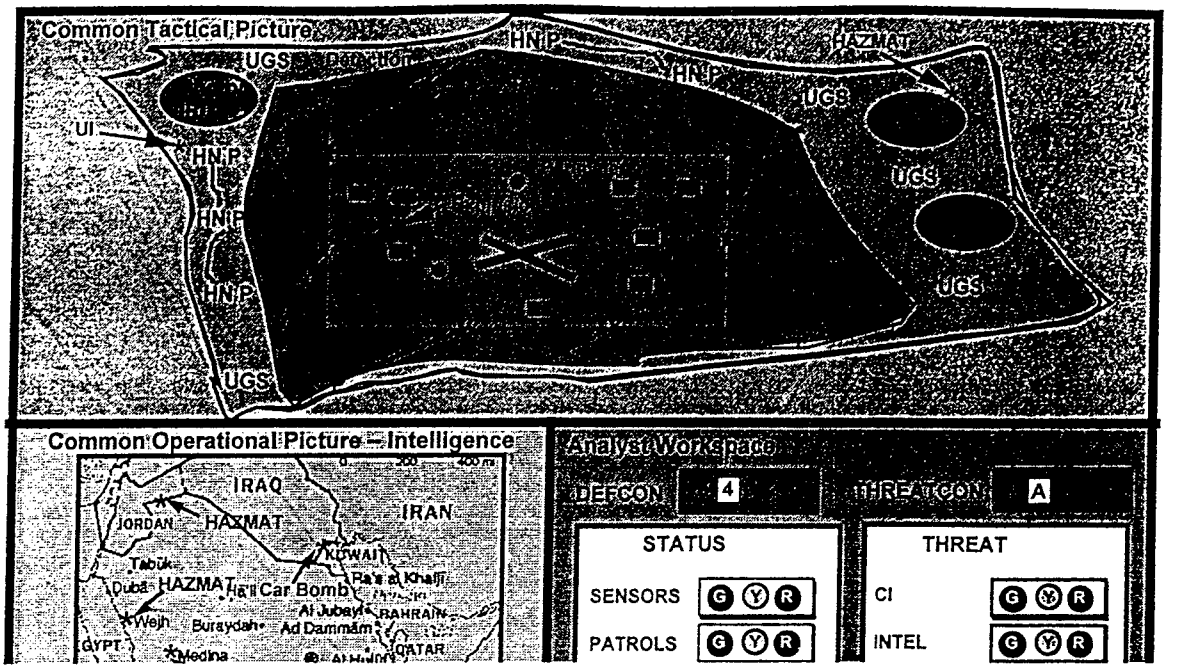

Common Tactical Picture
UGS
HNP
HAZMAT
UI
HNP
UGS
UGS
UGS
Common Operational Picture – Intelligence
IRAQ
IRAN
JORDAN
HAZMAT
KUWAIT
Tabuk
Dubai
HAZMAT
Ha'il Car Bomb
Ra's al Khafji
Al Jubayl
BAHRAIN
Ad Dammam
Wejh
Buraydah
QATAR
Medina
Analyst Workspace
DEFCON
4
THREATCON
A
STATUS
SENSORS
PATROLS
THREAT
CI
INTEL

Figure 3: Force Protection Common Operational Picture/Common Tactical Picture

Also contributing to the COP, would be the local installation's Common Tactical Picture (CTP). This is the coverage of the airman, perimeter, tactical, and detection zones around the base. It is envisioned that changes in the status of the base infrastructure (utilities) would be integrated with inputs from surveillance systems (such as the Tactical Automated Security System (TASS) and Unattended Ground Sensors (UGSs), Unpiloted Aerial Vehicles (UAVs), and patrols); intelligence and OSI reports; reports of local incidents and events (fires, explosions, subversion, medical alerts, etc.); information attacks; and host/local nation information to provide this CTP. The CTP from multiple installations throughout the region/theater would be a contributor to the COP. Additionally, the CTP would include local weather and base operational status, such as planned operations and runway usage.

Associated with maintenance of the Force Protection COP/CTP at the unit level is the analyst area of the COP/CTP display. This area provides support to the COP/CTP operator. It provides checklists, Standing Operating Procedures, position logs, and other support capabilities. Additionally, it eventually will provide rule or knowledge-based support for combining seemingly unrelated incidents/events into a meaningful entry for the CTP. It could also offer the opportunity to perform vulnerability and "what if" analyses.

It is envisioned that there would be possibly four components/anchor desks that would contribute to the CTP and benefit from its presentation of integrated information: Sensor Integration Cell, Intelligence/Counter Intelligence (Intel/CI) Cell, Base Status/Vulnerability Assessment Cell, Civil Military/External Cell. The Security Force (SF) battle manager would be located in the Base Defense Operations Center (BDOC) and would coordinate both the detection, identification, location, and characterization of the threat , as well as the response to a potential or actual action against the base.

It is envisioned that there would be possibly four components/anchor desks that would contribute to the CTP and benefit from its presentation of integrated information: Sensor Integration Cell, Intelligence/Counter Intelligence (Intel/CI) Cell, Base Status/Vulnerability Assessment Cell, Civil Military/External Cell. The Security Force (SF) battle manager would be located in the Base Defense Operations Center (BDOC) and would coordinate both the detection, identification, location, and characterization of the threat, as well as the response to a potential or actual action against the base.

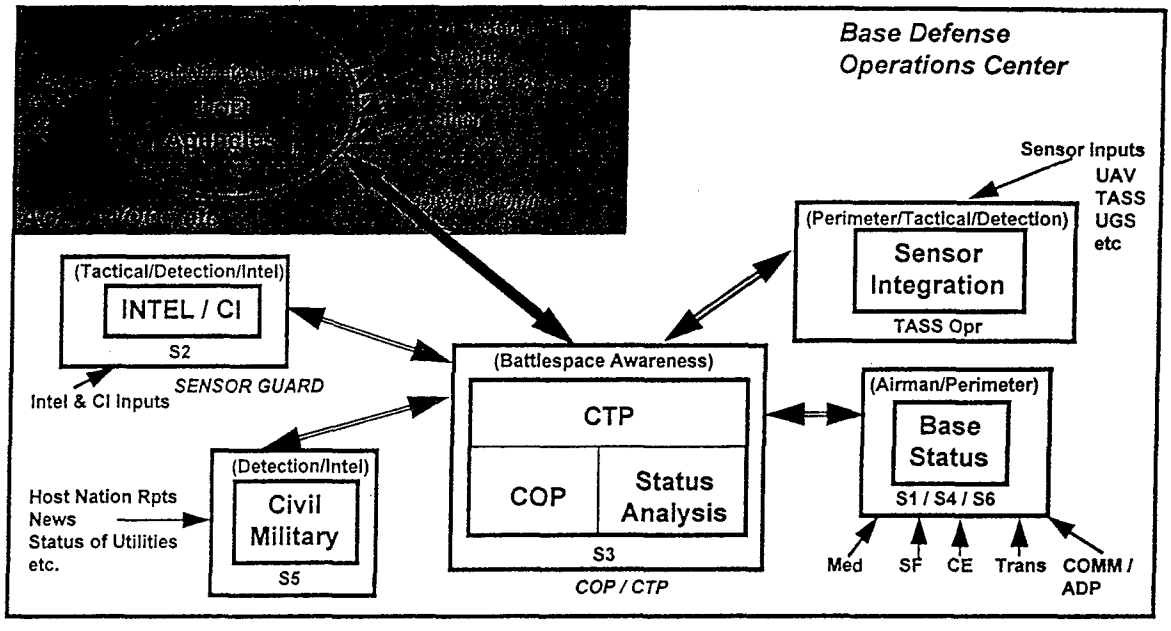


Figure 4: FP Battle Management C2: Unit Level

The Sensor Integration Cell (a permanent cell) would provide the situation awareness picture by the integration of the inputs from the supporting sensors systems, e. g., chem/bio detectors, TASS, UGS. This cell could task sensors to change coverage or add additional sensors. By controlling the sensors, it will be able to optimize coverage against potential types and locations of threats. Its contribution to the CTP would be the integrated Sensor Picture (Situation Awareness picture). The Intel/CI Cell (a permanent cell) would correlate the HUMINT and national sensor inputs, as well as facilitating the submission of Requests For Information (RFI) in support of the Collection Management process. It would be this cell's responsibility to task collection assets for additional information, query INTELINK/INTELINK-S for information, and query the various CI systems for additional information on terrorist and other groups/individuals. Its part of the CTP would be an adjunct to the Sensor Integration Cell input in order to clarify threat potential capabilities or threats in the area. The Base Status/Vulnerability Assessment Cell (possibly an "on call" cell) would be responsible for identifying and characterizing the critical infrastructures on the base that support base operations and the critical aspects of the base's mission. They would contribute information as to what areas need

protection and how they should be protected. This would affect the sensor coverage program managed by the Sensor Integration Cell. Additionally, once the Sensor Integration Cell and/or Intel/CI cell have characterized a threat, the Base Status Cell will be able to forecast intentions and areas of the infrastructure that are directly under attack or threat of attack and the impact of that attack. This cell would contribute annotated base diagrams/drawings and/or alerts (e. g., medical) to indicate infrastructure areas under actual or potential threat attack. The Civil Military/External Cell (possibly an "on call" cell) would provide information from the local police, other services, other bases, etc. that are external to the base which also may have a significant impact on the base's force protection. Its input to the CTP may be on the order of refugee movements, locations of disturbances or dissidents, other bases having attacks as a graphical overlay, status of host nation response assets (police, fire, disaster relief, etc.) and status of host nation utilities supporting the base or facility.

Development and Schedule:

Our basic approach for the development of this testbed capability is to use, as much as possible, COTS/GOTS products that are compatible with the Windows NT operating environment, per the request of our immediate user - the 820th Security Forces Group. Currently, our effort is divided into three phases so that we can continuously involve our user in our spiral development process and help the user to better define their requirements for this capability. The end goal is to use our collective experience from this testbed effort to publish a Request For Proposal for the productization of the Force Protection COP/CTP that will meet the needs of Security Force elements in any MAJCOM and, possibly the Joint arena. The following describes the phased development of this activity and anticipated completion dates. Phase I activity will be driven by the input of simulated data. The dates for phases II and II may change based on the immediate needs of the user and user operational requirements, as well as operator feedback on the previous phase's capabilities.

- Phase I: Initial Integration and CTP Development
SEP 98

- - Investigate the utility of advanced Mapping, Cartographic, and Geodesy (MC&G) capabilities and other display tools

- - Integration of the output of the TASS and tactical alerting and reporting system to provide the local situation awareness picture to create the Sensor Integration Cell

-- Start integration of Joint Warning and Reporting Network (JWARN) capability

- Phase II: COP Integration and Enhanced CTP Capability
SEP 99

-- Incorporate user feedback from Phase I to enhance the CTP

-- Investigate applicability and incorporation of multi-level security capabilities

-- Continue JWARN implementation, as it matures

-- Investigate integration with the Wing Command and Control System (WCCS)

-- Investigate incorporation of the Counter Intelligence Deployable System (CIDS) or other Counter Intelligence capabilities

-- Integrate SENSOR GUARD (a FP deployable intel capability) into the COP/CTP construct as the Intel/CI Cell

- Phase III: COP and CTP Enhancement SEP 00

-- Develop analyst support tools using rule-based or knowledge-based capabilities, timeline analysis capability, etc. for development of Analyst Area

-- Integrate JWARN control of CBR detectors into Sensor integration Cell

-- Integrate vulnerability assessment tools, medical reporting, SF reporting into Base Status Cell

-- Develop Civil Military/External Cell capability

Issues/Challenges:

- FP COP: As the Force Protection mission area matures, there will be a need for the FP COP to be defined and disseminated to the Security Forces within Theater in the same manner as the GCCS COP

- The FP COP/CTP must be brought under the umbrella of the GCCS as a Joint application. It should be a layer on the GCCS COP.

- Within the Air Force, the FP COP/CTP should be an application within Theater Battle Management Core System (TBMCS)

Future:

- The FP COP/CTP has applicability across all the services and should be made a Joint capability

- FP COP/CTP will be an experiment within the Expeditionary Forces Experiment - 99 in July 1999

Attachment: Definitions

Reference: CJCSI 3151.01, 10 June 1997, "Global Command and Control System Common Operational Picture Reporting Requirements"

Common Operational Picture. The COP is the integrated capability to receive, correlate, and display a Common Tactical Picture (CTP), including planning applications and theater-generated overlays/projections (i.e., Meteorological and Oceanographic (METOC), battleplans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data from JOPES, readiness data from SORTS, intelligence (including imagery overlays), reconnaissance data from the Global Reconnaissance Information System (GRIS), weather from METOC, predictions of nuclear, biological, and chemical (NBC) fallout, and Air Tasking Order (ATO) data.

Common Tactical Dataset. The CTD is a repository of data that contains all the information available to the JTF that will be used to build the COP and CTP. The CTD is not fused, correlated, or processed data in the sense that the information has not been scrutinized by the CCM [CINC COP Manager] or track managers for time value, redundancy, or conflicts. However, the CTD may contain processed intelligence data. The CTD is a major sub-component of the COP and refers to: the CINC designated repository for current battlespace information including disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war for the entire area of responsibility (AOR). Upon discretion of the CINC, the CTD may be a logical database vice physical if there are several JTFs or activities that will necessitate COP reporting. In these cases there may be more than one location of database storage.

Common Tactical Picture. The CTP is derived from the CTD and other sources and refers to the current depiction of the battlespace for a single operation within a CINCís AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real-time sensor information, and amplifying information such as METOC, SORTS [Status of Resources and Training System], and JOPES [Joint Operation Planning and Execution System].